1984, Hungarian Edition

verfassungsblog.de/1984-hungarian-edition-2/

Kim Lane Scheppele Di 18 Jun 2013

The Hungarian parliament recently passed a new national security law that enables the inner circle of the government to spy on people who hold important public offices. Under this law, many government officials must "consent" to being observed in the most intrusive way (phones tapped, homes bugged, email read) for up to two full months each year, except that they won't know which 60 days they are under surveillance.

Perhaps they will imagine they are under surveillance all of the time. Perhaps that is the point. More than 20 years after Hungary left the world captured in George Orwell's novel 1984, the surveillance state is back.

Now, if the Fidesz government of Prime Minister Viktor Orbán finds something it doesn't like – and there's no legal limit to what it may find objectionable – those under surveillance can be fired. The people at the very top of the government are largely exempt from surveillance – but this law hits their deputies, staffers and the whole of the security services, some judges, prosecutors, diplomats, and military officers, as well as a number of "independent" offices that Orbán's administration is not supposed to control.

The Orwellian aspirations of governments are obviously not confined to Hungary. The disclosure of two giant data collection programs carried out by the US National Security Agency shows that too many governments still aspire to know too much about too many people. I'm already on record as a critic of the American warrantless wiretapping programs, since I filed an amicus brief in Clapper v. Amnesty International, the case before the US Supreme Court this term that attempted to challenge the program. The US Supreme Court refused to grant the plaintiffs standing so the program has so far escaped judicial review. Many excellent legal analysts are writing about law underlying this program so I won't add to that in this post. For one particularly insightful and nonobvious take on the relevant law, see here.

Of course, one of the many negative consequences of the American surveillance program is that other governments will claim the right to follow in the US's footsteps. But an overreaching surveillance regime in the US does not justify a horrible copy elsewhere. I will concentrate in this post on the new Hungarian national security law, offered as a set of amendments to the 1995 law on the same topic, amendments which passed shortly before the US surveillance scandals broke.

Under Hungary's new national security law, certain authorized government officials may initiate intrusive surveillance on their higher-level underlings through asking for a surveillance order. Generating a surveillance order doesn't require that the target be suspected of doing anything illegal. Any old reason will do.

And who approves surveillance orders? No judicial warrants are needed. The only required approval comes from the Minister of Justice, a feature which keeps control of the program within the inner circles of the government. (Readers of my earlier posts may recall that this is the same person who has to approve much of the secret surveillance carried out by the Counter-Terrorism Police, or TEK.)

How can surveillance lead to a person being fired? The national security law creates a new qualification for whole series of jobs in the Hungarian government. All listed employees must now pass annual surveillance tests in order to remain in their jobs. Now that the law has passed, potential targets of surveillance must sign a "consent" form. If the targets have spouses, the spouses must sign consent forms, too. And if the targets or their spouses don't consent to this surveillance, the targets lose their jobs. In short, this "consent" is not optional and the whole family is fair game for surveillance.

The primary goal of this program appears to be gathering "dirt" on particular people and holding this information

against them when their superiors find it useful to do so. That may explain why the surveillance program collects the content of all communications as well as the results of audio and video monitoring inside people's homes, and the information may be stored for 20 years. Though the program allegedly evaluates people for fitness to work, the surveillance is not limited to what people do at work. Instead, it examines every detail of employees' lives "with a particular view to their behavior outside their employment, personal relationships, material or income status, or relationship with a person who, to their knowledge, has been sentenced for a criminal offence." So says the law. There are no provisions for the redaction of irrelevant information, something that would be hard to do with no definition of relevance in the law.

Who is now subjected to this surveillance requirement? Here's the list:

- Hungarian ambassadors and heads of consulates, anywhere in the world.
  Judges and prosecutors who work either with information gathered through secret surveillance or with information that might result in accepting a defendant's cooperation with the government in exchange for not being prosecuted (plea bargains).
- State commissioners, who are people appointed on an ad hoc basis to manage specific high-level tasks in the government.
- Deputy state secretaries, who are people working directly under government ministers and their state secretaries.
- Heads of the autonomous and self-regulating government agencies, a designation that includes the public procurement office, the office of economic competition, the equal treatment authority, the data protection office, national media council, the financial supervisory authority and the energy and public utilities authority.
- Heads of "government offices," their deputies and people of equivalent rank, a designation that includes regional offices of the central government, the central statistical office, national atomic energy agency, national office of intellectual property and the national tax and tariff office.
- Senior staff in the Parliament's central office.
- Senior staff in the office of the President of the Republic.
- The chief of the army, generals and others with equivalent rank.
- All heads of police departments (national, regional and local).
- All heads of state-owned companies.
- All employees of all of the security services, including the new Counter-Terrorism Police (TEK), the new Parliamentary Guard, the Office for the Protection of the Constitution (domestic intelligence), the Information Office (foreign intelligence), the National Security Expert Service (signals intelligence), the Military National Security Service, and the internal affairs unit of the police.

Since surveillance includes both sides of all communications, anyone who interacts with any of these people may have their words and deeds captured for 20 years as well. If state employees on this list are found to be doing something that the inner circle of the Fidesz government objects to, they can be classified as national security risks, a classification which disqualifies them from their jobs.

The surveillance is carried out by the National Security Expert Service (NSES) which has the technical capacity to wiretap, install bugs and intercept electronic communications. The law gives the Office for Constitutional Protection (OCP) responsibility for assessing the information collected in the surveillance sweeps to determine whether someone poses a danger to national security. Since all of the employees of both the NSES and the OCP can be put under intrusive surveillance themselves for up to two months each year, this must make for some interesting office politics.

When the OCP is finished with its assessment of each target of surveillance, it turns the results over to the official

who ordered the surveillance and that official makes the decision about whether the target is to be blacklisted. But the national security law provides no guidance either to the Office for Constitutional Protection or to the official who makes the decision because it does not indicate what they should be looking for or what procedures they must follow in making such determinations. Under the law, the targets of the surveillance have no right to appear at a hearing, nor do they have an opportunity to explain or provide additional evidence before the fateful determination is made. In fact, the targets won't even know when they are under surveillance or when the results are being assessed, so they can hardly insist on participating in a secret process. The law only says that the targets are to be informed when they have been blacklisted and given the reason why they have been so classified. But that reason may also be withheld from the target if the reason is classified as a state secret.

How may a state employee who has flunked the surveillance test get the assessment reconsidered? It depends on which office the person occupies. In general, the official at the top of the employee's workplace hierarchy can be asked to review the judgment. So, for example, if a blacklisted employee works in the central office of the Parliament or in the Parliamentary Guard, the Speaker of the Parliament can be asked to reconsider the classification; if the blacklisted person works in the office of the President of the Republic, the President can be asked to reassess the risk. The president of the National Judicial Office evaluates the blacklisted judges. The Chief Public Prosecutor evaluates the blacklisted prosecutors. Anyone working for the security services can appeal up to the Interior Minister.

The Prime Minister himself is the judge of last resort for the rest: the heads of the autonomous and self-regulating agencies, the heads of the government offices, diplomats, deputy state secretaries, state commissioners, military personnel, heads of the police and owners of state-owned enterprises.

According to the law, decisions at this ministerial level are final and cannot be appealed to any court.

Once a person has been blacklisted, however, she will no longer be eligible for her job. This will lead to a termination procedure through which the person is formally fired. But outcome of this procedure is not in doubt. The official who presides over the firing process will only be able to reach one conclusion: the blacklisted person must be fired because she no longer meets the qualifications for her job.

Any fired state employee can appeal her dismissal to a labor court. But since the decision to blacklist someone cannot be second-guessed by the labor court judge either, there is not much that the court can do. Judicial review of the procedure in these cases is very nearly meaningless.

Before someone moves into any of the positions that are flagged for the two-month surveillance each year, she must go through a background check, an elaborate process that can be carried out for up to 45 days. In addition to the jobs on the list above, government ministers, state secretaries and the members of Parliament who are on the intelligence committees must also go through a background check before they take office, even though they cannot be spied on again once they are in those jobs.

To begin the background check, the applicant fills in a questionnaire that requires, among other things, information about the foreign contacts of both the would-be job holder and the spouse. This then triggers a thorough investigation in which intelligence officers ask people for information about the target, gather information about the target from communications and data storage systems (like phone companies and internet service providers), record the person in public places, engage the target with secret informers, create fake organizations and documents to make the target believe she is interacting with someone else and engage in the disturbing option of "creating traps that do not cause physical harm." (A direct quote from the law.) Of course, if someone flunks the background check, then she doesn't get the job in the first place.

Those specifically exempted from either the background checks or the intrusive surveillance include the President of the Republic, the Prime Minister, Constitutional Court judges, the Speaker of the Parliament, the president of the Supreme Court (Curia), the president of the National Judicial Office, the Chief Public Prosecutor, the ombudsman and his deputies, the head of the data protection agency and members of the European Parliament.

The Hungarian government argues that the new national security law protects state secrets and guards against corruption. But the law doesn't limit the surveillance to looking for evidence of leaked secrets or bribes. Instead, anything that might be compromising seems to be in its remit. If the Hungarian government decides to fire a public official for having an extra-marital affair or refuses to appoint a public official who is too friendly with the political opposition, the national security law could provide cover.

Officials of the Hungarian government will say that what they are doing is nothing novel. Other countries, they will point out, have ways to determine whether high-level officials have played fast and loose with state secrets or whether people holding the public trust are corrupt. The US government has now been shown to be gathering up everyone's phone calls and emails, so how can anyone be critical of what the Hungarian government is doing?

I'm deeply critical of the US programs too, but the existence of the US programs should not give license for every other government on earth to spy on people without any concrete suspicion. Given that the Hungarian surveillance program involves listening to the content of phone conversations, reading emails and bugging the houses of state officials to see what they are doing, there are particular dangers here. What is to prevent the Hungarian government from simply blackmailing people with what they find? What keeps the Hungarian government from acting on purely political information (firing someone for criticizing the government, for example)? The law contains no meaningful protections against the use of the information for political and personal reasons and it offers no procedures that would reliably correct mistakes.

European Union law requires that the collection of personal information about individuals be examined by an independent data privacy officer who has the power to review government policies and actions in this area without fear of political interference. At the moment, the European Court of Justice has before it an infringement action brought by the European Commission that challenges the Hungarian government's firing of the previous data protection ombudsman, but the decision has not been announced. While the data privacy officer himself is on the list of persons exempted in the national security law, his office is still on the list of those whom the Prime Minister can put under surveillance. With this sort of legal ambiguity at the heart of the law, who is to oversee those who are collecting all of this information and who is to guarantee that these surveillance checks are not abused?

When Orwell wrote his famous novel in 1949 about the all-seeing surveillance state, the Cold War was rapidly closing in. Those on the eastern side of Europe were consigned to states in which personal privacy could never be taken for granted. A country that had been through that experience might be expected to have a particular sensitivity to what it means to turn citizens into spies against each other, especially a country whose leaders now pronounce their anti-communist sympathies at every turn. But the current Hungarian government seems to have learned little from its country's recent past. Those who refuse to learn from the past are doomed to repeat it. In Hungary, it is now approaching 1984 again.

This article was previously published on Paul Krugman's blog and is reposted here with kind permission by the author.

SUGGESTED CITATION Scheppele, Kim Lane: *1984, Hungarian Edition, VerfBlog,* 2013/6/18, http://verfassungsblog.de/1984-hungarian-edition-2/.